KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Stealthy PowerShell Backdoor Disguising as Windows Update

Tracker ID: TN1020 **Date:** 21/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

Background

A novel and fully undetected (FUD) PowerShell backdoor that conceals itself by masquerading as a Windows update procedure has been identified. The stealthy self-developed tool and related C2 instructions appear to be the product of a sophisticated, anonymous threat actor who has targeted around 100 victims in a covert operation. The malware and attack chains begin with a weaponized Microsoft Word document uploaded from Jordan on August 25, 2022.

Mistakes made by the threat actor led to its identification, which allowed the researchers to access and decrypt the encrypted C2 commands for each victim. The threat actor's mistakes led to its identification, allowing the researchers to obtain and decrypt the encrypted C2 orders for each victim. The initial intrusion vector is a LinkedIn-based spear-phishing attempt, according to metadata linked with the lure document, which ultimately results in the execution of a PowerShell script via some embedded macro code as a Windows update.

Before launching the scheduled task, the PowerShell script (Script1.ps1) connects to a remote command-and-control (C2) server to obtain a command that will be performed on the compromised system using a different PowerShell script (temp.ps1). However, the actor made an operational security mistake by using a basic incremental identifier (0, 1, 2, etc.) to individually identify each victim, allowing the C2 server orders to be reassembled.

In addition, researchers discovered that the list of active processes was exported, files in selected directories were listed, whoami was launched, and files in public user folders were deleted, among other significant activities. 32 security firms and 18 anti-malware engines have identified the fraudulent documents and PowerShell scripts as potentially harmful. The evidence was revealed at a time when Microsoft was making Excel 4.0 (XLM or XL4) and Visual Basic for Applications (VBA) macros inaccessible by default across Office products, forcing threat actors to use new delivery routes.

Indicators of Compromise

Please refer to the attached sheet for IOCs.

MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, Discovery, Command and Control.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Stealthy PowerShell Backdoor Disguising as Windows Update

Tracker ID: TN1020 **Date:** 21/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- As a protective measure, prevent unnecessary PowerShell execution by implementing policies and standards that permit only signed scripts to execute.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Verify the email sender and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link's target.
- Check the sender's identity. Unfamiliar email addresses, mismatched email and sender names, and spoofed company emails are some of the signs that the sender has malicious intent.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Tomer Bar, SafeBreach Labs Researchers Uncover New Fully Undetectable Powershell Backdoor, SafeBreach, 18th October 2022, External Link (safebreach.com)
- Ravie Lakshmanan, Experts Warn of Stealthy PowerShell Backdoor Disguising as Windows Update, The Hacker News, 19th October 2022, External Link (thehackernews.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Stealthy PowerShell Backdoor Disguising as Windows Update

Tracker ID: TN1020 **Date:** 21/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

*

URL	SHA256 Hash
hxxp://45.89.125.189/put	45f293b1b5a4aaec48ac943696302bac9c893867f1fc282e85ed8341dd2f0f50
hxxp://45.89.125.189/get	54ed729f7c495c7baa7c9e4e63f8cf496a8d8c89fc10da87f2b83d5151520514
	bda4484bb6325dfccaa464c2007a8f20130f0cf359a7f79e14feeab3faa62332
	16007ea6ae7ce797451baec2132e30564a29ee0bf8a8f05828ad2289b3690f5